

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

The email account yahya.al-ansari@yuttah.com, more
fully described in Attachment A.

Case No. MJ21-631

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, attached hereto and incorporated herein by reference.

located in the Eastern District of Michigan, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

50 U.S.C. § 4819(a)(2)(f)
18 U.S.C. § 1001

False statements to the Department of Commerce; false statements

The application is based on these facts:

- ☒ See Affidavit of Special Agent Jose Rodriguez, continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Jose Rodriguez, Special Agent

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 11/23/2021

Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, United States Magistrate Judge

Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
 COUNTY OF KING)

I, Jose Rodriguez, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUNDS

1. I am a Special Agent with the U.S. Department of Commerce (DOC), Bureau of Industry and Security (“BIS”), Office of Export Enforcement (OEE) presently assigned to the Portland Resident Office in Portland, Oregon. I have been a Special Agent since July 2013 and I have worked for BIS since November 2009. I am a graduate of the Federal Law Enforcement Training Center’s Criminal Investigator Training Program and I have received training in the investigation of crimes related to the violation of export laws.

2. As a result of my training and experience, I am familiar with federal laws and regulations governing the export of goods and technology from the United States, including the International Emergency Economic Powers Act (50 U.S.C. §§ 1701–1706), the Export Control Reform Act of 2018 (50 U.S.C. §§ 4801-4852 (ECRA) and the Export Administration Regulations (15 C.F.R. pts. 730–774) (EAR).

3. I submit this affidavit in support of an application for a search warrant under 18 U.S.C. § 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require A2 Hosting, Inc., 2000 Hogback Rd Ste 6, Ann Arbor, Michigan (hereinafter “Provider” or “A2”) to provide information, including the content of communications, associated with **yahya.al-ansari@yuttah.com** (the “**SUBJECT EMAIL ACCOUNT**”) which is further described in Attachment A to this affidavit. As set forth below, I have probable cause to believe that the **SUBJECT EMAIL ACCOUNT** contains evidence, as set forth in Attachment B to this affidavit, of violations of 50 U.S.C. § 4819(a)(2)(f) (false statements to the Department of Commerce) and 18 U.S.C. § 1001 (false statements).

4. This affidavit concerns an investigation conducted by the U.S. Department of Commerce (DOC), Bureau of Industry and Security (BIS), Office of Export Enforcement (OEE). The statements contained in this affidavit are based on information I have learned through my personal participation in this investigation, from oral and written reports of other law enforcement officers, from records, documents, and other evidence obtained during this investigation, and from my experience and training as a Special Agent. Since this affidavit is being submitted for the limited purpose of obtaining a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the authorization of the search warrant.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

6. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

7. This warrant application is to be presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

RELEVANT LAW

A. The Export Control Reform Act of 2018 (ECRA)

8. The ECRA provides, among its stated policy objectives, that “the national security and foreign policy of the United States require that the export, re-export, an in-country transfer of items, and specific activities of United States persons, wherever located, be controlled” 50 U.S.C. § 4811(2). To that end, the ECRA grants the President the authority “(1) to control the export, re-export, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or by foreign persons; and (2) the activities of United States persons, wherever located,

1 relating to” specific categories of items and information. 50 U.S.C. § 4812(b). The
2 ECRA further grants the Secretary of Commerce the authority to establish the applicable
3 regulatory framework.

4 9. Pursuant to ECRA, the DOC reviews and controls the export of certain
5 items, including commodities, software, and technologies, from the United States to
6 foreign countries through the Export Administration Regulations, 15 C.F.R. §§ 730-774.
7 In particular, the EAR restrict the export of items that could make a significant
8 contribution to the military potential of other nations or that could be detrimental to the
9 foreign policy or national security of the United States. The EAR impose licensing and
10 other requirements for items subject to the EAR to be lawfully exported from the United
11 States.

12 10. The most sensitive items subject to EAR controls are identified on the
13 Commerce Control List (CCL). 15 C.F.R. part 774, Supp. No. 1. Items on the CCL are
14 categorized by an Export Control Classification Number based on their technical
15 characteristics. Each Export Control Classification Number has export controls
16 requirements depending on destination, end use, and end user. The Commerce Country
17 Chart identifies which exports require a license based on the reasons for control under the
18 relevant Export Control Classification Number and the country of destination.

19 11. Commodities that are not assigned a particular Export Control
20 Classification Number are designated as “EAR99.” Items designated as EAR99 require a
21 license for export to Cuba, Iran, North Korea, or Syria unless a license exception applies.
22 In addition, DOC maintains an Entity List (Supplement 4 to Part 744 of the EAR)
23 identifying persons and entities for which an export license is required, separate and apart
24 from license requirements arising from the Commerce Country Chart.

25 12. Under Title 50, United States Code Section 4819(a)(2)(f), no person may
26 make any false or misleading representation, statement, or certification, or falsify or
27 conceal any material fact, to the Department of Commerce in the course of an action
28 subject to the EAR, or for the purpose of or in connection with effecting any export,

1 reexport, or in-country transfer of an item subject to the Export Administration
2 Regulations.

3 13. Under Title 50, United States Section 4819(b), “[a] person who willfully
4 commits, willfully attempts to commit, or willfully conspires to commit, or aids and abets
5 in the commission of, an unlawful act described in subsection (a),” shall be subject to
6 criminal penalties.

7 **B. Section 1001**

8 14. Under Title 18, United States Code, Section 1001(a), it is a crime to
9 knowingly and willfully (1) falsify, conceal, or cover up by any trick, scheme, or device a
10 material fact; (2) make any materially false, fictitious, or fraudulent statement or
11 representation; or (3) make or uses any false writing or document knowing the same to
12 contain any materially false, fictitious, or fraudulent statement or entry.

13 **C. The Iranian Transactions and Sanctions Regulations (ITSR)**

14 15. The Iranian Transactions and Sanctions Regulations (ITSR) impose, among
15 other prohibitions, the following prohibition, set forth in 31 C.F.R. § 560.204—
16 Prohibition of any Sale or Supply of any Goods, Technology, Services to Iran or the
17 Iranian Government: “Except as otherwise authorized [by a license issued by
18 OFAC]¹, the exportation . . . sale, or supply, directly or indirectly, from the United States,
19 or by a United States person, wherever located, of any goods, technology, or services to
20 Iran or the Government of Iran is prohibited”

21 **SUMMARY OF INVESTIGATION**

22 16. Law enforcement has probable cause to believe that Yahya Al-Ansari,
23 Production Manager, Yuttah FZE (Yuttah), located in Sharjah, United Arab Emirates,
24 provided false and misleading statements to BIS’s Export Control Officer (ECO) during a
25 post-shipment verification related to an export and attempted export of accelerometers

26 _____
27 ¹ The Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury
28 administers the ITSR and may issue licenses authorizing transactions that would otherwise be
prohibited under the ITSR.

1 subject to the EAR, further described below in more details. OEE has been investigating
 2 illicit diversion of these accelerometers to China and Iran for military end-uses and
 3 suspects Yuttah's accelerometer shipments will be diverted to a prohibited destination.

4 **SUMMARY OF PROBABLE CAUSE**

5 **A. Background Information on Yuttah FZE**

6 17. Yuttah is located in the Sharjah International Airport Free Zone (warehouse
 7 A4-53, SAIF Zone, 500001 Sharjah) in the United Arab Emirates. On their website,
 8 www.yuttah.com, Yuttah describes itself as a leading manufacturer of sensor solutions.
 9 Based on the BIS's ECO visit, further discussed below, Yuttah's business location
 10 consisted of a front office area and a single-bay warehouse workshop in the back and
 11 alongside of the office. The front office was also very hot in temperature and relatively
 12 undisturbed, which suggested to the ECO it had been unoccupied for a period of time.
 13 The warehouse office did not appear like the office building as depicted as on their
 14 website, www.yuttah.com. The website portrayed a complex and vibrant operation with
 15 multiple manufacturing lines and manufacturing equipment.

16 18. Al-Ansari told the ECO that he had recently completed five years of
 17 education and training in Germany as an electrical engineer and that he had worked with
 18 companies while in Germany.

19 **B. The Accelerometers**

20 19. The accelerometers discussed in this affidavit are manufactured by a
 21 company in the Western District of Washington (the Company) and shipped from the
 22 Western District of Washington by the Company to its destination or a foreign
 23 distributor. Pursuant to Section 15 of the Code of Federal Regulations, Part 744.21,
 24 *Restrictions on certain 'military end use' or 'military end user' in Burma, The People's*
 25 *Republic of China, The Russian Federation, or Venezuela*, in June 2018, the Deputy
 26 Assistant Secretary of Commerce for Export Administration established a licensing
 27 requirement for these accelerometers. The company received a written notification of
 28 these licensing requirements; the Company in turn informed its distributors and

customers of that requirement. Initially, the requirement applied only to some exports to China (those for significant contribution to military systems), but the requirement was subsequently amended in December 2018 to cover all exports to China. Generally, and for other destinations, these accelerometers are designated EAR99 and do not require a license to be exported to most destinations. They would require a license for embargoed countries such as Iran and North Korea or prohibited end-use or end-users. The United Arab Emirates is a known transshipment country to Iran. BIS has an Export Control Officer based in Dubai, United Arab Emirates, in part, to counter illicit diversion in the United Arab Emirates.

20. I have been investigating and preventing diversion of these accelerometers to China since the establishment of the licensing requirement. I am also familiar with the product, the market patterns in ordering the product, and the ways prohibited end-users (or their agents) have been attempting to circumvent the licensing requirement. I have visited with the Company to understand their business, how they also use their accelerometers to fabricate other sensor modules, and the type of manufacturing equipment needed. Most recently, between February and May 2021, I disrupted a Belgium-German network that was diverting these accelerometers to China.

C. Detention and Post-Shipment Verification

21. On June 24, 2021, I was advised by Customs and Border Protection (CBP) Seattle of a high-value shipment of the accelerometers from the Company to Yuttah FZE. The shipment was for 600 accelerometers, with a total value \$93,600. I contacted the Company for additional details. The Company provided the invoice and an end-user form², and notified me of a smaller prior shipment to Yuttah, on or around June 9, 2021,

² An “end-user form” collects information about the intended end-use of the product and parties to the transaction that might not be identified in the invoice or purchase order. It facilitates the seller’s due diligence requirements by helping the seller vet the transaction for prohibited end-use or end-users. The form can be a proprietary document created by the seller or manufacturer, or an official BIS -711 form. The BIS 711 form, however, is a signed certification by Consignee or Purchaser, that reads in part “We acknowledge that the making of any false statements or

1 of 92 units valued at \$17,572. I requested that CBP detain the June 24th shipment for
2 inspection. I also requested that the Dubai ECO complete a post-shipment verification to
3 confirm the disposition of the June 9th shipment and end-use of the current shipment.

4 22. BIS's Dubai ECO met with Al-Ansari and his father on July 27, 2021, at
5 Yuttah's office and manufacturing facility. According to the ECO, the father is listed as
6 the company's Director. They informed the ECO that their target customers are located
7 locally, in Abu Dhabi, as well as overseas in India. Al-Ansari also claimed that they are
8 working through his contacts in Europe to generate business in that market as well. Al-
9 Ansari did not provide any specific names for their customers. Al-Ansari stated that they
10 do not ship to China because China already has cheaper versions of their sensor modules.
11 Al-Ansari claimed that Yuttah is a relatively new manufacturing company that started
12 business in October 2020. When asked about the prior shipment, Al-Ansari said they
13 bought them for inventory and to manufacture their sensor modules and discussed some
14 of the sensor modules they claim to manufacture. He later provided the ECO with a link
15 for the product and specifications via email, using SUBJECT EMAIL ACCOUNT.

16 23. The ECO toured the warehouse and observed approximately 6 empty
17 workstations with wooden tops, none of which appeared to contain any electrostatic
18 damage (ESD) signage or equipment. The workstations were sitting on an unmarked,
19 seemingly untreated concrete floor. The inside of the warehouse was oriented in an L-
20 shaped configuration. The warehouse was much smaller than the warehouse depicted in
21 pictures appearing on their website. Moreover, the warehouse had a fraction of the
22 workspaces depicted on the website. According to the ECO, the warehouse was
23 drastically different than what the website depicted. During the tour, the father had a table
24 with some samples of the sensor muddles they claim to be manufacturing. The father
25 showed the ECO one open metal housing for a sensor module, but there were no

26 _____
27 concealment of any material fact in connection with this statement may result in imprisonment or
28 fine, or both and denial, in whole or in part, of participation in U.S. exports and reexports". The
Company collected both forms from Yuttah for these transactions.

AFFIDAVIT OF Rodriguez - 7

USAO# 2021R01334

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1 accelerometers placed in it. The ECO did not observe completed sensor modules or items
2 ready for shipping. The ECO did not observe any testing or calibration equipment at the
3 warehouse, and ultimately determined Yuttah to be an unreliable recipient of U.S. origin
4 items.

5 24. Based on my experience investigating these types of cases and in my
6 experience interacting with the Company, ESD workspaces are needed to manufacture
7 sensors using the accelerometers. Absent an ESD workspace, small and common ESD
8 discharges can damage the accelerometer. Testing and calibration equipment is also
9 required to complete the production of the sensor modules they claim to manufacture at
10 the location.

11 25. The lack of equipment observed by the ECO is not compatible with the
12 claims they make in their website or answers provided to the ECO. Based on my
13 experience conducting these investigations, I believe that Yuttah is buying the
14 accelerometers for a third party as their facilities do not show the capability of being able
15 to integrate the accelerometers. Although Yuttah claimed they just opened 8 months ago
16 and are still developing their business, in my experience, in this industry the normal
17 business practice would have been to buy the capital equipment necessary to integrate
18 raw materials before purchasing the raw materials.

19 26. Yuttah's investment of over \$111,000 on just one type of accelerometer, in
20 light of the total lack of capital equipment necessary to integrate that accelerometer, is
21 consistent with a front company operation. Yuttah's website shows multiple sensor
22 modules with different ratings. For example, the sensor module explained to the ECO by
23 Yuttah has 9 distinct ratings. Each sensor module needs 1 to 3 accelerometers of the same
24 rating. Each accelerometer is also capable of only one rating. The accelerometers Yuttah
25 bought are of a single rating, and so cannot be used for the other 8 ratings specified in
26 their specifications sheet. Yuttah did not purchase any other accelerometers of other
27 ratings from the Company, nor did Yuttah appear to have other inventory from other
28 manufacturers at their warehouse. That is, Yuttah would appear to be unable to fulfill

1 requests for their own advertised range of sensor modules even if they had the equipment
2 necessary to do so. Based on my experience in analyzing the Company's sales, the
3 number of accelerometers Yuttah procured are typical for an organization that has used
4 and validated the accelerometer for their final product. Normally, a company would order
5 1-3 units to integrate into their sensor and would then scale up the orders once they had
6 validated the particular accelerometer as compatible with their module. Based on the lack
7 of equipment or finished product observed by the ECO, it is unlikely that Yuttah had
8 completed that phase.

9 27. The very first order from Yuttah was 92 units; a few weeks later, they
10 ordered another 600 units. The Company did ask Yuttah where Yuttah had previously
11 obtained parts and whether Yuttah had tested the Company's parts. Yuttah
12 representatives deflected that question by providing a specification sheet of the final
13 sensor module they wanted to manufacture using the Company's accelerometers. Even
14 the smaller order of 92 accelerometers is, in my experience, a relatively large order, and
15 would have been ordered by a company with an established manufacturing line, which is
16 not what the ECO observed.

17 28. The ECO also asked about Jack Millner. Millner was the first person that
18 contacted the Company on or around May 26, 2021. Using the email account
19 jack.millner@yuttah.com, Millner corresponded for multiple days with a Company sales
20 representative to place the initial order and transmit the end-user forms. During the ECO
21 visit, Al-Ansari told the ECO that Yuttah also retained "freelance" sales representatives
22 who work remotely to procure and sell their products, and that Millner was one of
23 Yuttah's sales representatives. Based on my experience investigating illicit accelerometer
24 procurements (including ongoing investigations), the timing of Millner's email, and the
25 lack of any firmer connection between Millner and Yuttah, I suspect Millner was a fake
26 persona or a person related to the recently disrupted Belgium-German network.

27 29. I asked the ECO to send some follow-up questions to Yuttah. On July 28,
28 2021, the ECO sent a follow-up question about Millner. Al-Ansari, using the **SUBJECT**

1 **EMAIL ACCOUNT**, responded that Millner *"Is a university student doing part time*
2 *with us for small tasks as per our instructions and has no decision making (mini job)."*

3 30. The Company provided a copy of email exchanges they had with Yuttah on
4 their original electronic form. I proceeded to analyze the email headers for three
5 accounts: the email account used by Millner, Al-Ansari's **SUBJECT EMAIL**
6 **ACCOUNT**, and the email account info@yuttah.com (this was another email account
7 used to correspond with the Company). The email headers appeared to show a single
8 device as the source of all the emails. Because the emails had different Internet Protocol
9 (IP) addresses, in my experience, that is consistent with a mobile device or a laptop. I
10 requested further official analysis of the emails.

11 31. On August 27, 2021, I received a report from BIS's National Computer
12 Forensics Laboratory that confirmed the emails were originating from a single device.
13 The report states that each email's header indicates the email was sent from a device with
14 the hostname of "LAPTOP6MRPMF0R". The report looked at emails from the account
15 used by Millner, the **SUBJECT EMAIL ACCOUNT**, and the account
16 info@yuttah.com.

17 32. Based on those findings, I determined that Al-Ansari was misleading the
18 ECO as to who Millner was and recommended that CBP seize the shipment based on the
19 misleading information provided to BIS.

20 **D. Petition Filed by Al-Ansari**

21 33. Throughout September 2021, CBP processed the June 24th shipment seizure
22 and notified Yuttah via email. Al-Ansari filed a petition seeking relief. Because Al-
23 Ansari did not provide further documentation in its petition, and based on our
24 recommendation based on the misleading statements, CBP denied relief.

25 34. On October 21, 2021, Al-Ansari filed a supplemental petition with CBP
26 and it was referred to my office. I informed Al-Ansari that I will reconsider my
27 recommendation to CBP if he, among other things:
28

- Provided documents that confirm the disposition of the initial shipment sent by the Company.
- Provided Jack Millner's resume and contact information.

35. On October 28, 2021, Al-Ansari responded using the **SUBJECT EMAIL ACCOUNT**. He asked for clarification on what type of documents I was requesting, to which I wrote we needed the invoice, packing list, and inventory control records that would help account for the initial shipment of accelerometers. With regards to Millner, Al-Ansari wrote:

"NO CV AVAILABLE. It is a Virtual Customer Service Agent, everyone in the company access it. This business model is nothing new and is a trend applied in most companies nowadays to assure fast response and standardization. Anyway, I am exclusively the employee in the company dedicated to resolve this issue."

36. The description of Millner as a "Virtual Customer Service Agent" rather than a real person is in contradiction to the answers provided to the BIS ECO during the post-shipment verification in person and via email. Further, Millner was not providing or being used as customer service representative when placing the order or negotiating terms with the Company. The statements about Millner validates that Al-Ansari is providing deceptive answers to the government questions.

37. In response to the request for specific documents, on October 28, 2021, Al-Ansari wrote:

"Mr. Rodriguez,
We confirmed several times, the items were not resold. No invoices or packing lists available."

38. Al-Ansari has not provided to the ECO, CBP or me documents or records confirming the disposition of the first shipment of accelerometers. When asked, he consistently refers the government to Yuttah's website or states they have not been resold.

1 39. Every single accelerometer shipped by the Company contains a serial
2 number. In my experience, working with the Company and hundreds of site-visits I have
3 performed with other manufacturers, resellers or service centers, serial numbers are used
4 for traceability, regulatory requirements, warranty issues, or industry standards associated
5 with quality and control. Every single serial number is recorded in the Company's
6 invoice. Customers that manufacture sensor modules like those that Yuttah claims to
7 manufacture will record the serial numbers used in each sensor module they manufacture.
8 Even if Yuttah does not practice industry standards, it would need to keep an inventory of
9 sensors produced for basic accounting purposes. Yuttah has not provided, even when
10 asked, such an inventory.

11 40. When Al-Ansari filed its supplemental petition, on October 21, 2021, he
12 also wrote directly to BIS and me using the **SUBJECT EMAIL ACCOUNT**. The
13 originating IP address of this message was 46.114.95.82. Based on open-source IP
14 address locators, that IP address returns to Telefonica Germany GmbH & Co. OHG,
15 located in Offenburg, Germany. This is the first time any of the Yuttah's email IP
16 addresses, analyzed by me, returned outside the UAE. The device that was identified in
17 the email header was "LAPTOP6MRPMF0R", the same device used for the other emails
18 discussed.

19 41. Based on my training and experience, I believe Al-Ansari's deceptive
20 statements are intentional and consistent with an attempt to obfuscate the real destination
21 of the shipment of accelerometers. Since Al-Ansari himself stated he is the only
22 employee dealing with this issue, and because all emails sent from Yuttah are associated
23 with a mobile device (likely a laptop) he is apparently using, I believe the content of his
24 emails in his account will show for whom he is procuring the accelerometers on these
25 two orders, or will contain other evidence of their ultimate destination.

26 42. Yuttah pre-paid both orders. Al-Ansari would likely have sought
27 confirmation of the order with its customer or co-conspirator prior to spending over
28 \$111,000. Moreover, Al-Ansari would likely have coordinated with the customer or co-

1 conspirator to receive the funds for the purchase. Further, the delay on the second order
 2 on June 24, 2021, which is now seized, would have created a scenario where Al-Ansari
 3 likely needed to communicate with the customer or co-conspirator to justify the delays of
 4 the delivery. Therefore, I also believe communications between the implicated parties
 5 will also be found on the **SUBJECT EMAIL ACCOUNT**.

6 **E. Nature of documents sought and background regarding email services**

7 43. The domain yuttah.com is registered with A2 Hosting, Inc. In my training
 8 and experience, I have learned that companies like A2 provide a variety of web services
 9 for a fee. On their website, A2 discusses the range of services provided, which include
 10 website hosting services and email hosting services. A2 services are customizable and
 11 include virtual private servers or dedicated servers. A virtual private server is a shared
 12 server with allocated space for multiple companies, while a dedicated server is a specific
 13 server with a determined size for the exclusive use of one customer. I performed a
 14 commercially available query on the domain name “yuttah.com” in order to determine
 15 the mail exchanger record, which specifies the mail server responsible for accepting
 16 messages on behalf of a domain name. I identified the mail exchange for “yuttah.com”
 17 as “barracuda.supercp.com,” and more specifically “supercp.com”. According to the
 18 same commercial query, the “supercp.com” server is also hosted by A2.³

19 44. No preservation order has been served on A2 for the **SUBJECT EMAIL**
 20 **ACCOUNT**.

21 45. Based on my training and experience with other email providers, when the
 22 subscriber sends an email, it is initiated at the user’s computer, transferred via the Internet
 23

24
 25 ³ I reviewed A2 Hosting support information to understand why “barracuda.supercp.com” (rather
 26 than the customer domain, “yuttah.com”) was being used by A2 Hosting as the mail exchange
 27 server. I determined that the “barracuda.supercp.com” mail exchange is associated with an
 28 additional service provided by A2 to manage email spam. According to the A2 Hosting website,
 when the Barracuda Spam Firewall is enabled, the domain’s MX (mail exchanger) record must
 also be updated. Therefore, the “barracuda.supercp.com” serves as preliminary server to control
 email spam, but ultimately forwards the email to the customer domain.

1 to A2's servers, and then transmitted to its end destination. Depending on the level of
2 service paid for by the user, a copy of the email will be saved on the virtual private server
3 or a dedicated server. Unless the sender of the e-mail specifically deletes the e-mail from
4 the A2 server, the email can remain on the system indefinitely. Even if the sender deletes
5 the email, it may continue to be available on A2's servers for a certain period of time.

6 46. A sent or received email typically includes the content of the message,
7 source and destination addresses, the date and time at which the email was sent, and the
8 size and length of the email. If an email user writes a draft message but does not send it,
9 that message may also be saved by A2's server but may not include all of these categories
10 of data.

11 47. In general, email hosting companies providers like A2 ask each of their
12 subscribers to provide certain personal identifying information when entering into a
13 service contract. This information can include the subscriber's full name, physical
14 address, telephone numbers and other identifiers, alternative e-mail addresses, and, for
15 paying subscribers, means and source of payment (including any credit or bank account
16 number). In my training and experience, such information may constitute evidence of the
17 crimes under investigation because the information can be used to identify the account's
18 user or users.

19 48. Email providers typically retain certain transactional information about the
20 creation and use of each account on their systems. This information can include the date
21 on which the account was created, the length of service, records of log-in (i.e., session)
22 times and durations, the types of service utilized, the status of the account (including
23 whether the account is inactive or closed), the methods used to connect to the account
24 (such as logging into the account via A2 website), and other log files that reflect usage of
25 the account. In addition, e-mail providers often have records of the Internet Protocol
26 address ("IP address") used to register the account and the IP addresses associated with
27 particular logins to the account. Because every device that connects to the Internet must
28

1 use an IP address, IP address information can help to identify which computers or other
2 devices were used to access the e-mail account.

3 49. In some cases, e-mail account users will communicate directly with an e-
4 mail service provider about issues relating to the account, such as technical problems,
5 billing inquiries, or complaints from other users. E-mail providers typically retain
6 records about such communications, including records of contacts between the user and
7 the provider's support services, as well records of any actions taken by the provider or
8 user as a result of the communications. In my training and experience, such information
9 may constitute evidence of the crimes under investigation because the information can be
10 used to identify the account's user or users.

11 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

12 50. Pursuant to Title 18, United States Code, Section 2703(g), this application
13 and affidavit for a search warrant seeks authorization to permit A2 Hosting, Inc., and its
14 agents and employees, to assist agents in the execution of this warrant. Once issued, the
15 search warrant will be presented to A2 with direction that it identify the account
16 described in Attachment A to this affidavit, as well as other subscriber and log records
17 associated with the account, as set forth in Section I of Attachment B to this affidavit.

18 51. I anticipate executing this warrant under the Electronic Communications
19 Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by
20 using the warrant to require A2 Hosting, Inc. to disclose to the government copies of the
21 records and other information (including the content of communications) particularly
22 described in Section I of Attachments B. Upon receipt of the information described in
23 Section I of Attachments B, government-authorized persons will review that information
24 to locate the items described in Section II of Attachments B.

25 52. Analyzing the data contained in the forensic image may require special
26 technical skills, equipment, and software. It could also be very time-consuming.
27 Searching by keywords, for example, can yield thousands of "hits," each of which must
28 then be reviewed in context by the examiner to determine whether the data is within the

1 scope of the warrant. Merely finding a relevant “hit” does not end the review process.
 2 Keywords used originally need to be modified continuously, based on interim results.
 3 Certain file formats, moreover, do not lend themselves to keyword searches, as keywords,
 4 search text, and many common e-mail, database and spreadsheet applications do not store
 5 data as searchable text. The data may be saved, instead, in proprietary non-text format.
 6 And, as the volume of storage allotted by service providers increases, the time it takes to
 7 properly analyze recovered data increases, as well. Consistent with the foregoing,
 8 searching the recovered data for the information subject to seizure pursuant to this
 9 warrant may require a range of data analysis techniques and may take weeks or even
 10 months. All forensic analysis of the data will employ only those search protocols and
 11 methodologies reasonably designed to identify and seize the items identified in Section II
 12 of Attachment B to the warrant.

13 53. Based on my experience and training, and the experience and training of
 14 other agents with whom I have communicated, it is necessary to review and seize a
 15 variety of e-mail communications, chat logs and documents, that identify any users of the
 16 subject account and e-mails sent or received in temporal proximity to incriminating e-
 17 mails that provide context to the incriminating communications.

18 **REQUEST FOR NONDISCLOSURE AND SEALING**

19 54. The government requests, pursuant to the preclusion of notice provisions of
 20 Title 18, United States Code, Section 2705(b), that A2 Hosting, Inc. be ordered not to
 21 notify any person (including the subscriber or customer to which the materials relate) of
 22 the existence of this warrant for such period as the Court deems appropriate. The
 23 government submits that such an order is justified because notification of the existence of
 24 this Order would seriously jeopardize the ongoing investigation. Such a disclosure would
 25 give the subscriber an opportunity to destroy evidence, change patterns of behavior,
 26 notify confederates, or flee or continue his flight from prosecution. Indeed, the target of
 27 the investigation is based in the United Arab Emirates, and he would be far less likely to
 28 travel outside of the UAE were he to know that he was under investigation.

1 55. It is further respectfully requested that this Court issue an order sealing,
2 until further order of the Court, all papers submitted in support of this application,
3 including the application and search warrant. I believe that sealing this document is
4 necessary because the records relate to an ongoing investigation that includes foreign
5 targets. Premature disclosure of the contents of this affidavit and related documents may
6 have a significant and negative impact on the continuing investigation and may severely
7 jeopardize its effectiveness.

8 //

9 //

10 //

CONCLUSION

56. On the basis of my participation in this investigation and the information summarized above, I submit that there is probable cause to believe that evidence of violations of 50 U.S.C. § 4819(a)(2)(f) (false statements to the Department of Commerce) and 18 U.S.C. § 1001 (false statements), as more fully described in Attachment B, is presently contained in the **SUBJECT EMAIL ACCOUNT** (the account yahya.al-ansari@yuttah.com), which is more fully described above and in Attachment A. I therefore request that the Court issue a warrant authorizing a search of the aforementioned account, described in Attachment A, for the items listed in Attachment B, and the seizure and examination of any such items found. Because the warrant will be served on Provider, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.



Jose Rodriguez, Affiant
Special Agent
U.S. Department of Commerce

SUBSCRIBED AND SWORN before me this 23rd day of November, 2021.



THE HONORABLE BRIAN A. TSUCHIDA
United States Magistrate Judge

ATTACHMENT A

Account to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following account:

- **yahya.al-ansari@yuttah.com**

(“SUBJECT EMAIL ACCOUNT”) as well as all other subscriber and log records associated with the account, which are located at premises owned, maintained, controlled or operated by A2 Hosting, Inc. (“Provider”), an e-mail provider headquartered at 2000 Hogback Rd Ste 6, Ann Arbor, Michigan.

ATTACHMENT B**I. Information to be disclosed by A2 Hosting, Inc. (“Provider”), for search:**

1. To the extent that the information described in Attachment A is within the possession, custody, or control of Provider, regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all e-mails associated with the account yahya.al-ansari@yuttah.com (the “SUBJECT EMAIL ACCOUNT”) from January 1, 2021 to the present (including email, attachments, and embedded files), including stored or preserved copies of e-mails sent to and from the accounts, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;

b. The contents of all e-mails sent by yahya.al-ansari@yuttah.com on behalf of a different email account.

c. All records or other subscriber information regarding the identification of the accounts, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the accounts were created, the length of service, the IP address used to register the accounts, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

1 e. All records or other information stored by an individual using the
2 account, including address books, contact and buddy lists, calendar data, pictures, and
3 files, including:

4 f. All records pertaining to communications between the Provider and any
5 person regarding the accounts, including contacts with support services and records of
6 actions taken.

7
8 Provider is hereby ordered to disclose the above information to the government within
9 14 days of service of this warrant.

10
11 **II. Information to be seized by the government:**

12 All information described above in Section I that constitutes fruits, evidence, or
13 instrumentalities of violations of 50 U.S.C. § 4819(a)(2)(f) (false statements to the
14 Department of Commerce) or 18 U.S.C. § 1001 (false statements), those violations occurring
15 between April 1, 2021 and the present, including, for each account or identifier listed on
16 Attachment A, information pertaining to the following matters:

17 a. All records, data, and communications reflecting or relating to the
18 shipment of accelerometers from the United States;

19 b. All records, data, and communications reflecting or relating to work
20 order MFG-WO-2021-22470;

21 c. All records, data, and communications reflecting or relating to Purchase
22 Order PUR-ORD-2021-22401 and PUR-ORD-2021-22401;

23 d. All records, data and communications between the SUBJECT EMAIL
24 ACCOUNT and Jack Millner;

25 e. All records, data, and communications reflecting or relating to reselling,
26 transferring, or buying accelerometers on behalf of a third party;

27 f. All records necessary to determine the value of any U.S.-controlled
28 content in foreign products manufactured by Yuttah;

1 g. All records, data and communications relating to the preparation of
2 export documents or end-user forms or customs form the United States to a foreign
3 country;

4 h. All records, data, and communications reflecting or relating to U.S.
5 export control laws and regulations;

6 i. All records, data, and communications reflecting or relating identifying
7 aiders, abettors' facilitators, coconspirators, or witnesses regarding the subject offenses;

8 j. All messages, documents, and profile information, attachments, or other
9 data that serves to identify any persons who use or access the SUBJECT EMAIL
10 ACCOUNT, or who exercise in any way any dominion or control over the SUBJECT
11 EMAIL ACCOUNT;

12 k. Any address lists or buddy/contact lists associated with the SUBJECT
13 EMAIL ACCOUNT;

14 l. All subscriber records associated with the SUBJECT EMAIL
15 ACCOUNT, including name, address, local and long distance telephone connection
16 records, or records of session times and durations, length of service (including start date)
17 and types of service utilized, telephone or instrument number or other subscriber number
18 or identity, including any temporarily assigned network address, and means and source of
19 payment for such service) including any credit card or bank account number;

20 m. Any and all other log records, including IP address captures, associated
21 with the specified account;

22 n. Any records of communications between Provider and any person about
23 issues relating to the SUBJECT EMAIL ACCOUNT, such as technical problems, billing
24 inquiries, or complaints from other users about the specified account. This to include
25 records of contacts between the subscriber and the provider's support services, as well as
26 records of any actions taken by the provider or subscriber as a result of the
27 communications.
28

1 o. Information identifying accounts that are linked or associated with the
2 SUBJECT EMAIL ACCOUNT.
3
4

5 This warrant authorizes a review of electronically stored information seized, copied, or
6 disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities
7 described in this warrant. The review of this electronic data may be conducted by any
8 government personnel assisting in the investigation, who may include, in addition to law
9 enforcement officers and agents, attorneys for the government, attorney support staff, and
10 technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the
11 seized, copied, or disclosed electronic data to the custody and control of attorneys for the
12 government and their support staff for their independent review.
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by A2 Hosting, Inc., and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of A2 Hosting, Inc.. The attached records consist of _____ (pages/CDs/megabytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of A2 Hosting, Inc., and they were made by A2 Hosting, Inc. as a regular practice; and

b. such records were generated by A2 Hosting, Inc.'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of A2 Hosting, Inc. in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by A2 Hosting, Inc., and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature